МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

Зам. директора по учебной работе
ИСТиД (филиал) СКФУ в г. Пятигорске
_____ М.В. Мартыненко
«__» _____ 2020 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

ПРОЕКТНО-ТЕХНОЛОГИЧСЕКАЯ ПРАКТИКА

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	Очная
Год начала обучения	2020
Изучается	в 6 семестре

СОГЛАСОВАНО:
Зав. выпускающей кафедрой систем управления и информационных технологий
_____ И.М. Першин
«__» _____ 2020 г.

Представитель работодателя:

начальник отдела технической защиты информации ЗАО «Контур-Сервис ТВ»
_____ А.С. Ермаков

«__» _____ 201_ г.

Рассмотрено УМК
Протокол №___ от «___»_____

Председатель УМК ИСТиД (филиал) СКФУ в г. Пятигорске
_____А.Б. Нарыжная

РАЗРАБОТАНО:
Зав. кафедрой систем управления и информационных технологий
_____ И.М. Першин
«__» _____ 2020 г.

Старший преподаватель кафедры систем управления и информационных технологий
_____ И.В. Калиберда
«__» _____ 2020 г.

Пятигорск, 2020

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

Зам. директора по учебной работе
ИСТиД (филиал) СКФУ в г. Пятигорске
_____ М.В. Мартыненко
«__» _____ 2020 г.

ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПРОЕКТНО-ТЕХНОЛОГИЧСЕКАЯ ПРАКТИКА

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	Очная
Год начала обучения	2020
Изучается	в 6 семестре

СОГЛАСОВАНО:
Зав. выпускающей кафедрой СУиИТ
_____ И.М. Першин
«__» _____ 2020 г.

Представитель работодателя:

начальник отдела технической защиты информации ЗАО «Контур-Сервис ТВ»
_____ А.С. Ермаков

«__» _____ 2020 г.

Рассмотрено УМК
Протокол №___ от «___»_____

Председатель УМК ИСТиД (филиал) СКФУ в г. Пятигорске
_____А.Б. Нарыжная

РАЗРАБОТАНО:
Зав. кафедрой систем управления и информационных технологий
_____ И.М. Першин
«__» _____ 2020 г.

Старший преподаватель кафедры систем управления и информационных технологий
_____ И.В. Калиберда
«__» _____ 2020 г.

Пятигорск, 2020

1. **Цели практики**

Целями производственно-технологической практики по направлению подготовки 10.03.01 Информационная безопасность являются:

- закрепление, расширение, углубление и систематизация знаний, полученных при изучении дисциплин профиля подготовки;
- приобретение практических навыков и компетенций в сфере профессиональной деятельности;
- подбор необходимого материала для выполнения для дальнейшей проработки темы выпускной квалификационной работы.

2. **Задачи практики**:

Задачами производственно-технологической практики являются:

1) Изучить:
- современные аппаратные и программные средства вычислительной техники;
- принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны;
- конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации;
- потенциальные каналы утечки информации, способы их выявления и методы оценки опасности;
- основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации;
- методы и средства инженерно-технической защиты информации;
- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- принципы построения современных криптографических систем, стандарты в области криптографической защиты информации;
- основные правовые положения в области информационной безопасности и защиты информации.

2) Освоить:
- методы организации и управления деятельности служб защиты информации на предприятии;
- технологии проектирования, построения и эксплуатации комплексных систем защиты информации;
- методы научных исследований уязвимости и защищенности информационных процессов;
- методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

3) Подобрать, изучить и обобщить научно-техническую литературу, нормативно-методические материалы по инженерно-технической защите информации. Научиться внедрять комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации, в том числе сравнительного анализа типовых криптосхем. Разработать предложения по совершенствованию и повышению эффективности применяемых мер на основе анализа результатов контрольных проверок, изучения и обобщения опыта эксплуатации объекта информатизации. Участвовать в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям

защиты информации по соответствующим классам безопасности. Знать вопросы нормирования, организации и оплаты труда, вопросы обеспечения безопасности жизнедеятельности на предприятии.

3. Место практики в структуре образовательной программы

Производственно-технологическая практика относится к блоку 2 «Практики», ее освоение происходит в 6-м семестре. Практика базируется на следующих дисциплинах. практиках: «Методы проектирования систем технической охраны объектов информатизации», «Защита и обработка конфиденциальных документов», «Научно-исследовательская работа», «Технологическая практика».

Для освоения программы практики, обучающиеся должны владеть следующими знаниями и компетенциями:

- способностью к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности;
- использованием на практике умений и навыков в организации исследовательских и проектных работ, в управлении коллективом.

Результаты прохождения практики могут быть использованы в дальнейшем в подготовке выпускных квалификационных работ.

4. Вид, тип практики, способ и формы ее проведения

Вид практики: производственная;
Тип практики: проектно-технологическая;
Способ проведения практики: выездная или стационарная.
Форма проведения практики: непрерывно.

5. Место и время проведения практики

Проектно-технологическая практика может проводиться в сторонних организациях или на кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.

Производственно-технологическая практика проводится в 6 семестре, продолжительностью 4 недели.

6. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

6.1 Наименование компетенций

Индекс	Формулировка:
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
ОК-8	способностью к самоорганизации и самообразованию
ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
ПК-7	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-8	способностью оформлять рабочую техническую документацию с учетом действующих

	нормативных и методических документов
ПК-9	способностью осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
ПК-11	способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации
ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ПСК-5	способностью разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение
ПСК-6	способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности

6.2 Знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций

Формируемые компетенции	Вид работы обучающегося на практике	Планируемые результаты обучения при прохождении практики, характеризующие этапы формирования компетенций		
		Навыки или практический опыт деятельности	Умения	Знания
ОК-5	Знакомство с коллективом организации, с его деятельностью и нормативными документами	Владеть методикой проверки защищенности объектов информатизации на соответствие требованиям нормативных документов	Обобщать научно-техническую литературу, нормативно-методические материалы по инженерно-технической защите информации	Знать вопросы нормирования, организации и оплаты труда, вопросы обеспечения безопасности жизнедеятельности на предприятии
ОК-8	Самостоятельное знакомство и анализнормативных документов, связанных с защитой информации на данном предприятии	Владеть методикой исследования защищенности объектов информатизации от утечки информации	Подбирать, научно-техническую литературу по инженерно-технической защите информации	Знать основные правовые положения в области информационной безопасности и защиты информации
ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособност и и эффективности применяемых программных, программно-	владеть в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и	принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и	знать и принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств

	аппаратных и технических средств защиты информации	технических средств защиты информации	технических средств защиты информации	защиты информации
ПК-7	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	владеть анализом исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	знать анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-8	Знакомство с локальными документами, связанными с защитой информации на данном предприятии	Владеть методикой изучения локальных документов защищенности объектов от утечки информации на предмет их соответствия нормативной документации	Оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знать рабочую техническую документацию с учетом действующих нормативных и методических документов
ПК-9	Составление краткого отчета об уровне защищенности данного предприятия от утечки информации	Владеть методами составления обзора по вопросам обеспечения информационной безопасности	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, по профилю своей профессиональной деятельности	Знать методы и приемы подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по профилю своей профессиональной деятельности
ПК-12	Проведение анкетирования работников организации с целью исследования системы защиты информации	Владеть навыками обработки экспериментальных данных	Уметь проводить экспериментальные исследования системы защиты информации	Знать методы и приемы проведения экспериментальных исследований системы защиты информации
ПК-13	Принимать участие в проведении экспериментальных исследований системы защиты информации	Владеть навыками обработки экспериментальных исследований системы защиты информации	Уметь проводить экспериментальные исследования системы защиты информации	Знать методы и приемы проведения экспериментальных исследований системы защиты информации
ПК-15	Организовывать технологический процесс защиты	Владеть навыками организации процесса защиты	Уметь работать с нормативными документами	Знать методы и приемы подбора, изучения и обобщения научно-

	информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю		технической литературы, нормативных и методических материалов по профилю своей профессиональной деятельности
ПСК-5	Разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Владеть приемами выбора, организации внедренияи последующего сопровождение необходимых технологий и технических средств	Уметь разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации	Знать принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
ПСК-6	Утвердить сформированный комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности с руководством организации	Владеть приемами расчета экономической целесообразности проекта	Уметь внедрять комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации, в том числе сравнительного анализа типовых криптосхем	Знать современные аппаратные и программные средства вычислительной техники

6.3.Соответствие планируемых результатов видам профессиональной деятельности

Планируемые результаты сформулированы в соответствии с профессиональным стандартом «Специалист по технической защите информации», утвержден приказом Министерства труда и социальной защиты Российской Федерации от «1» ноября 2016г. № 599н.

Виды профессиональной деятельности выпускника в соответствии с ОП	Задачи профес-сиональной деятельности выпускника	Трудовые функции	Вид работы студента на практике	Реализуемые компетенции (в соответствии с ОП)
проектно-технологическая	сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;	Проектирование объектов в защищенном исполнении	составление краткого отчета об уровне защищенности данного предприятия от утечки информации	ОК-5, ОК-8, ПК-6, ПК-7, ПК-8, ПК-9, ПК-12, ПСК-5, ПСК-6
	проведение проектных расчетов элементов систем обеспечения информационной безопасности;	Проектирование объектов в защищенном исполнении	изучить и обобщить опыт эксплуатации объекта информатизации	ПСК-5, ПСК-6
	участие в разработке технологической и эксплуатационной документации;	Проектирование объектов в защищенном исполнении	разработка подсистемы управления информационной безопасностью для отдельной структуры организации	ОК-5, ОК-8, ПК-6, ПК-7, ПК-8, ПК-9, ПК-12, Пк-13,Пк-15ПСК-5, ПСК-6
	проведение предварительного технико-экономического обоснования проектных расчетов;	Проектирование объектов в защищенном исполнении	утвердить сформированный комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности с руководством организации	ОК-5, ОК-8, ПК-6, ПК-7, ПК-8, ПК-9, ПК-12, ПСК-5, ПСК-6
	сбор, изучение научно-	Проведение аттестации	знакомство с коллективом	ОК-5, ОК-8

	технической информации, отечественного и зарубежного опыта по тематике исследования;	объектов на соответствие требованиям по защите информации	организации, с его деятельностью и нормативными документами	
экспериментально-исследовательская;	проведение экспериментов по заданной методике, обработка и анализ их результатов;	Проведение аттестации объектов на соответствие требованиям по защите информации	проведение анкетирования работников организации с целью исследования системы защиты информации	ОК-5, ОК-8, ПК-6, ПК-7, ПК-8, ПК-9, ПК-12, ПСК-5, ПСК-6
	проведение вычислительных экспериментов с использованием стандартных программных средств;	Проведение сертификационных испытаний средств защиты информации на соответствие требованиям по безопасности информации	обработка экспериментальных данных, полученных при анкетировании	ОК-5, ОК-8, ПК-6, ПК-7, ПК-8, ПК-9, ПК-12, ПСК-5, ПСК-6
организационно-управленческая.	осуществление организационно-правового обеспечения информационной безопасности объекта защиты;	Организация и проведение работ по технической защите информации	расчет экономической целесообразности проекта	ПСК-6
	организация работы малых коллективов исполнителей;	Организация и проведение работ по технической защите информации	организация внедрения и последующего сопровождение разработанного проекта	ПСК-5
	участие в совершенствовании системы управления информационной безопасностью;	Организация и проведение работ по технической защите информации	внедрение комплексной системы и отдельных специальных технических и программно-математических средств защиты информации на объекте информатизации	ПСК-6
	изучение и	Организация и	знакомство с	ОК-5, ОК-

	обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;	проведение работ по технической защите информации	локальными документами, связанными с защитой информации на различных предприятиях определенной отрасли	8, ПК-6, ПК-7, ПК-8, ПК-9, ПК-12, ПСК-5, ПСК-6
	контроль эффективности реализации политики информационной безопасности объекта защиты.	Проведение аттестации объектов на соответствие требованиям по защите информации	изучение современных аппаратных и программных средства вычислительной техники	ОК-5, ОК-8, ПК-6, ПК-7, ПК-8, ПК-9, ПК-12, ПСК-5, ПСК-6

7. Объем практики

Объем занятий: Итого 81 ч. 3 з.е.
Продолжительность 2 недели
Зачет с оценкой 6 семестр

8. Структура и содержание практики

Разделы (этапы) практики	Реализуемые компетенции	Виды работ обучающегося на практике	Количество часов	Формы текущего контроля
Начальный этап	ОК-5, ОК-8, ПК-6, ПК-7, ПК-8, ПК-9, ПК-12, ПСК-5, ПСК-6	Сбор, обработка и систематизация фактического материала Изучение организационно-правовой структуры объекта исследования. Анализ объекта исследования на предмет комплексной защиты информации.	27	
Промежуточный этап	ОК-5, ОК-8, ПК-6, ПК-7, ПК-8, ПК-9,	Сбор, обработка и систематизация	27	

	ПК-12, 13,15ПСК-5, ПСК-6	фактического и литературного материала Наблюдения, измерения Самостоятельная работа		
Заключительный этап	ОК-5, ОК-8, ПК-6, ПК-7, ПК-8, ПК-9, ПК-12, ПСК-5, ПСК-6	Составление отчета по практике Формирование предложений Публичная защита отчета	27	Публичная защита выполненной работы, по итогом, которой выставляется зачет с оценкой

9. Формы отчетности по практике

1. Дневник
2. Отчет обучающегося
3. Отзыв руководителя практики от вуза

Структура отчета

1. Задания

_____

_____

2. Индивидуальное задание

_____

_____

3. Список использованной литературы
4. Приложения (при необходимости).

10. Технологическая карта самостоятельной работы обучающегося

Коды реализуемых компетенций	Вид деятельности обучающегося	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ОК-5, ОК-8	Сбор материалов по структуре предприятия, правил документооборота	отчет	Собеседование	11	2	13
ПК-9, ПСК-5	Подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по инженерно-	отчет	Устный опрос	11	2	13

	технической защите объектов информатизации					
ПК-6, ПК-7, ПК-8, ПК-12,13,15	проведение экспериментов по заданной методике, обработка и анализ результатов.	отчет	Собеседование	11	2	13
ПСК-5, ПСК-6	сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности.	отчет	Устный опрос	11	2	13
ПСК-5, ПСК-6	Предложения по совершенствованию системы управления информационной безопасностью.	отчет	Собеседование	11	2	13
ПСК-5, ПСК-6	Оформление отчёта по практике.	отчет	Защита отчета оценкой	14	2	16
Итого за 6 семестр				**69**	**12**	**81**
Итого				**69**	**12**	**81**

11. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

Фонды оценочных средств, позволяющие оценить уровень сформированностикомпетенций, размещен в УМК производственно-технологичсекой практики на кафедре СУиИТ и представлен следующими компонентами:

11.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Паспорт фонда оценочных средств

Код оцениваемой компетенции	Этап формирования компетенции	Средства и технологии оценки	Тип контроля	Вид контроля	Наименование оценочного средства
ОК-5, ОК-8, ПК-6, ПК-7, ПК-9,12,13,15 ПСК-5, ПСК-6	Начальный	собеседование	текущий	текущий	Задания для проверки уровня знаний

ПК-6, ПК-7, ПК-8, ПК-12,13,15 ПСК-5, ПСК-6	Промежуточный	Собеседование	текущий	текущий	Задания для проверки уровня умений и навыков
ПК-6, ПК-7, ПК-8, ПК-12,13,15 ПСК-5, ПСК-6	Заключительный	Защита отчета	промежуточный	промежуточный	Задания на практику

11.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Уровни сформированности компетенций	Индикаторы	Дескрипторы			
		2 балла	3 балла	4 балла	5 баллов*
Базовый	**Знать:** принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны; потенциальные каналы утечки информации, способы их выявления и методы оценки опасности; основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации; методы и средства инженерно-технической защиты информации;	Отсутствует знания: принципов организации информационных систем в соответствии с требованиям информационной защищенности и в соответствии с требованиями по защите государственной тайны; потенциальных каналов утечки информации, способов их выявления и методы оценки опасности; основной номенклатуры и характеристик аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации; методов и средств инженерно-технической	Имеются знания: принципов организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны; потенциальных каналов утечки информации, способов их выявления и методы оценки опасности; - основной номенклатуры и характеристик аппаратуры, используемой для перехвата и анализа	Знает: принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны; потенциальные каналы утечки информации, способы их выявления и методы оценки опасности; основную номенклатуру и характеристик аппаратуры, используемой для перехвата и анализа сигналов в технических каналах	

		защиты информации;	сигналов в технических каналах утечки информации методов и средств инженерно-технической защиты информации	утечки информации; методы и средства инженерно-технической защиты информации;	
	Уметь: подбирать, обобщать научно-техническую литературу, нормативно-методические материалы по инженерно-технической защите информации; внедрять комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации	Отсутствует умения: подбирать, обобщать научно-техническую литературу, нормативно-методические материалы по инженерно-технической защите информации; внедрять комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации	Имеются умения: подбирать, обобщать научно-техническую литературу, нормативно-методические материалы по инженерно-технической защите информации; внедрять комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации	Умеет: подбирать, обобщать научно-техническую литературу, нормативно-методические материалы по инженерно-технической защите информации; внедрять комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации	
	Владеть: методами организации и управления деятельностью служб защиты информации на предприятии; технологией проектирования, построения и эксплуатации комплексных систем защиты информации;	Отсутствует навыки владения: методами организации и управления деятельностью служб защиты информации на предприятии; технологией проектирования, построения и эксплуатации комплексных систем защиты информации	Имеются навыки владения: методами организации и управления деятельностью служб защиты информации на предприятии; технологией проектирования, построения и эксплуатации	Владеет: методами организации и управления деятельностью служб защиты информации на предприятии; технологией проектирования, построения и эксплуатации комплексных систем защиты	

			комплексных систем защиты информации	информации;	
Повышенный	**Знать:** принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; принципы построения современных криптографических систем, стандарты в области криптографической защиты информации; основные правовые положения в области информационной безопасности и защиты информации;				Знает: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; принципы построения современных криптографических систем, стандарты в области криптографической защиты информации;
	Уметь: разрабатывать предложения по совершенствованию и повышению эффективности применяемых мер по защите информации, на основе анализа результатов контрольных проверок				Умеет: разрабатывать предложения по совершенствованию и повышению эффективности применяемых мер на основе анализа результатов контрольных проверок
	Владеть: методикой проверки защищенности объектов информатизации на соответствие требованиям нормативных				Владеет: методикой проверки защищенности объектов информатизации на соответствие

	документов.				требованиям нормативных документов.

11.3. Критерии оценивания компетенций

Оценка *«отлично»* выставляется студенту, если:

- знает, как решать практические задачи в области информационной безопасности и имеет практические навыки.
- знает, как решать практические задачи повышенной сложности в области информационной безопасностии имеет практические навыки.
- способен выполнять решения практических задач в области информационной безопасности в полном объеме, полностью способен к самостоятельному выполнению решения практических задач в области информационной безопасности.
- способен выполнять решения практических задач повышенной сложности в области информационной безопасностив полном объеме, полностью способен к самостоятельному выполнению решения практических задач в области информационной безопасности.

Оценка «*хорошо*» выставляется студенту, если:

- имеются знания практических задач в области информационной безопасности, но навыки реализуются недостаточно.
- имеются знания практических задач в области информационной безопасности, но навыки реализуются недостаточно.
- умеет решать практические задачи в области информационной безопасности.

Оценка «*удовлетворительно*» выставляется студенту, если:

- знания практических задач в области информационной безопасностиимеются, но практических навыков нет.
- демонстрирует понимание значимости практических задач в области информационной безопасности. Испытывает затруднения в решении практических задач в области информационной безопасности.
- знания практических задач в области информационной безопасностиимеются, но практических навыков нет.

Оценка «*неудовлетворительно*» выставляется студенту, если:

- отсутствуют знания практических задач в области информационной безопасности.
- отсутствуют знания практических задач в области информационной безопасности.
- отсутствие способности для решения практических задач в информационной безопасности. Не умеет решать практические задачи в области информационной безопасности.

11.4. Описание шкалы оценивания

Максимальная сумма баллов по **практике** устанавливается в **100** баллов и переводится в оценку по 5-балльной системе в соответствии со шкалой:

Шкала соответствия рейтингового балла 5-балльной системе

Рейтинговый балл	**Оценка по 5-балльной системе**
88 – 100	Отлично
72 – 87	Хорошо
53 – 71	Удовлетворительно
<53	Неудовлетворительно

11.5 Типовые контрольные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения ОП

Задания, позволяющие оценить знания, полученные на практике (базовый уровень)

Контролируемые компетенции или их части (код компетенции)	Формулировка задания	
Общекультурные компетенции (ОК):		
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;	Задание 1	Основные понятия (категории) в области государственной тайны.
	Задание 2	Перечень сведений, составляющих государственную тайну, и сведений, которые не подлежат засекречиванию.
ОК-8 способностью к самоорганизации и самообразованию;	Задание 1	Изучение основных видов нормативно-правовой документации в сфере информационной безопасности.
	Задание 2	Изучение организационно-правовой документации предприятия (устав, положение о предприятии и т.д.)
Профессиональные компетенции (ПК):		
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;	Задание 1	Изучение технической документации.
	Задание 2	Изучение методических документов по защите информации.
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;	Задание 1	Аудит информационной безопасности предприятия.
	Задание 2	Обзор современных средств защиты информации.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Задание 1	Проведение анкетирования работников на предмет информационной безопасности предприятия.
	Задание 2	Первичная статистическая обработка анкет.
Профессиональные специальные компетенции (ПК):		
ПСК-5 способностью разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Задание 1	Обзор технических средств и необходимых для их установки технологий.
	Задание 2	Изучение правил внедрения и адаптации систем безопасности.
ПСК-6 способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.	Задание 1	Модель информационной безопасности.
	Задание 2	Основные составы преступлений в сфере информации.

Задании, позволяющие оценить знания, полученные на практике (повышенный уровень)

Контролируемые компетенции или их части		Формулировка задания	
Код компетенции	Формулировка		
Общекультурные компетенции (ОК):			
		Задание 1	Разработка политики информационной безопасности предприятия.
		Задание 2	Аудит информационной безопасности, основные направления деятельности и этапы проведения аудита.
ОК-8 способностью к самоорганизации и самообразованию		Задание 1	Способы коммерческого шпионажа и обеспечения защиты от него.
		Задание 2	Политика информационной безопасности компании.
Профессиональные компетенции (ПК):			
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;		Задание 1	Защита информации от утечки по акустическим каналам и за счет микрофонного эффекта.
		Задание 2	Защита информации от утечки по электромагнитным каналам.
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;		Задание 1	Основные категории в области коммерческой тайны.
		Задание 2	Законное и незаконное получение информации, составляющей коммерческую тайну.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации		Задание 1	Защита информации от утечки по техническим каналам.
		Задание 2	Защита информации от утечки по визуально-оптическим каналам.
Профессиональные специальные компетенции (ПК):			
ПСК-5 способностью разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение		Задание 1	Криптографические средства защиты информации.
		Задание 2	Пресечение разглашения конфиденциальной информации.
ПСК-6 способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.		Задание 1	Шифрование речи.
		Задание 2	Технологии использования паролей.

Задания, позволяющие оценить умения и навыки, полученные на практике (базовый уровень)

Контролируемые компетенции или их части		Формулировка задания
Код компетенции	Формулировка	

Общекультурные компетенции (ОК):		
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;	Задание 1	Аппаратные средства защиты информации.
	Задание 2	Программные средства защиты информации.
ОК-8 способностью к самоорганизации и самообразованию;	Задание 1	Защита от несанкционированного доступа и копирования.
	Задание 2	Обеспечение информационной безопасности средствами Windows XP.
Профессиональные компетенции (ПК):		
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;	Задание 1	Организационная защита информации.
	Задание 2	Инженерно-техническая защита информации.
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;	Задание 1	Организационные мероприятия.
	Задание 2	Организационно-технические и технические мероприятия.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Задание 1	Классификация угроз в сфере защиты информации.
	Задание 2	Меры обеспечения информационной безопасности.
Профессиональные специальные компетенции (ПК):		
ПСК-5 способностью разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Задание 1	Принципы обработки персональных данных.
	Задание 2	Защита интеллектуальной собственности.
ПСК-6 способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.	Задание 1	Допуск к государственной тайне.
	Задание 2	Основные категории в сфере защиты персональных данных.

Задания, позволяющие оценить умения и навыки, полученные на практике (повышенный уровень)

Контролируемые компетенции или их части		Формулировка задания	
Код компетенции	Формулировка		
Общекультурные компетенции (ОК):			
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой		Задание 1	Защита данных в MicrosoftOffice 2007, 2010.
		Задание 2	Использование цифровой подписи. Понятие компьютерного вируса. История

мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;		возникновения и причины появления компьютерных вирусов.
ОК-8 способностью к самоорганизации и самообразованию;	Задание 1	Разновидности вирусов. Уязвимость программ и пути проникновения вирусов.
	Задание 2	Принципы работы антивируса, разновидности антивирусных программ и основные меры защиты от вирусов.
Профессиональные компетенции (ПК):		
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;	Задание 1	Разработка технической документации на основании существующих в организации документов.
	Задание 2	Разработка методических документов по защите информации и доведение их до сведения персонала организации.
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;	Задание 1	Решение усложненных задач профессиональной деятельности на основе информационной и библиографической культуры.
	Задание 2	Владение навыками применения информационно-коммуникационных технологий в конкретных ситуациях.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Задание 1	Уверенное применение механизмов использования аппаратных средств и программного обеспечения.
	Задание 2	Уверенное применение процедур и результатов использования аппаратных средств и программного обеспечения.
Профессиональные специальные компетенции (ПК):		
	Задание 2	Уверенное применение различных способов обеспечения информационной безопасности.
ПСК-5 способностью разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Задание 1	Уверенное применение на практике технических средств по защите информации при помощи необходимых для их установки технологий.
	Задание 2	Умение тестировать компоненты систем защиты информации при помощи различных методик.
ПСК-6 способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.	Задание 1	Проактивные системы защиты, системы контроля целостности и системы отражения атак.
	Задание 2	Блокирование несанкционированного доступа к компьютеру и принцип действия брандмауэра.

11.6. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

На каждом этапе практики осуществляется текущий контроль за процессом формирования компетенций. Предлагаемые обучающемуся задания позволяют проверить компетенции: ОК-5, ОК-8, ПК-6, ПК-7, ПК-8, ПК-9, ПК-11, ПК-12, ПК-13, ПК-15,ПСК-5, ПСК-6.

Задания предусматривают овладение компетенциями на разных уровнях: базовом и повышенном. Для продвинутого уровня, предусмотрены, задания повышенной сложности.

При организации и проведении производственной практики необходимо:

- на начальном этапе провести анализ предметной области по теме исследования, провести сбор и обработку материалов по теме исследования – 27 час.
- на промежуточном этапе разработать техническое задание по теме исследования – 27 час.
- на заключительном этапе провести анализ полученных результатов, формирование предложений по теме исследования - 27 час.

Структура отчета проведенных научных исследований: введение; аналитический обзор по теме исследования; разработка программ и методик проведения исследований; заключение; список использованных источников.

Рекомендуемые формы по оформлению материалов отчета представлены в приложениях к настоящим указаниям.

При проверке задания, оцениваются:

–грамотно составленный аналитический отчет;

–последовательность изложения материала;

–грамотная формулировка актуальности рассматриваемых выработанных предложений;

–постановка и решение проблемы по теме научного исследования.

При защите отчета оцениваются:

–знания современных средств, видов и методик систем информационной безопасности;

–знания технологии умение их при решении практических задач при решении практических задач;

–выводы и предложения по результатам выполненной работы.

12. Методические рекомендации для обучающихся по прохождению практики

На первом этапе необходимо ознакомиться со структурой практики, обязательными видами работ и формами отчетности, которые отражены в Методических указаниях по практике.

Для успешного выполнения заданий по преддипломной практике, обучающемуся необходимо самостоятельно детально изучить представленные источники литературы

№ п/п	Вид самостоятельной работы	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая	Интернет-ресурсы
1	Сбор материалов по структуре предприятия, правил документооборота	1,2	1,2	1	1,2
2	Подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по инженерно-технической защите объектов информатизации, современным аппаратным и программным средствам защиты информации, а так же подбор материала в	1,2	1,2	1	1,2

	соответствии с выбранной тематикой дипломного проектирования.				
3	проведение экспериментов по заданной методике, обработка и анализ результатов.	1,2	1,2	1	1,2
4	сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности.	1,2	1,2	1	1,2
5	совершенствование системы управления информационной безопасностью.	1,2	1,2	1	1,2
7	Оформление отчёта по практике.	1,2	1,2	1	1,2

13. Учебно-методическое, информационное и материально-техническое обеспечение практики

13.1. Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики

13.1.1. Перечень основной литературы:

1. Методы проектирования систем технической охраны объектов : лабораторный практикум / сост. И.В. Калиберда ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 129 с. - Библиогр. в конце глав.
2. Лонцева И.А. Основы научных исследований [Электронный ресурс]: учебное пособие/ Лонцева И.А., Лазарев В.И.— Электрон. текстовые данные.— Благовещенск: Дальневосточный государственный аграрный университет, 2015.— 185 с.— Режим доступа: http://www.iprbookshop.ru/55906.— ЭБС «IPRbooks», по паролю

13.1.2. Перечень дополнительной литературы

1. Методы проектирования систем технической охраны объектов : учеб. пособие / П.П. Мулкиджанян, Ю.Г. Айвазов, В.В. Родишевский и др. ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 163 с. - Прил.: с. 83-159. - Библиогр.: с. 82.
2. Кришталюк А.Н. Конфиденциальное делопроизводство и защита коммерческой тайны [Электронный ресурс]: курс лекций/ Кришталюк А.Н.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 199 с.— Режим доступа: http://www.iprbookshop.ru/33427.— ЭБС «IPRbooks», по паролю.

13.1.3. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по практике:

1. Методические указания по организации и проведению производственно-технологической практики для студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность».

13.1.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://elibrary.ru - Научная электронная библиотека eLIBRARY.RU
2. http://www.biblioclub.ru -Университетская библиотека online

14. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем
Информационные технологии:

- Мультимедийные технологии: проекторы, ноутбуки, персональные компьютеры, комплекты презентаций, учебные фильмы.
- Дистанционная форма консультаций во время прохождения конкретных этапов практики и подготовки отчета, которая обеспечивается: выходом в глобальную сеть Интернет, поисковыми системами Яндекс, Мейл, Гугл, системами электронной почты.
- Компьютерные технологии и программные продукты: Электронная-библиотечная система (ЭБС) IPRboks.ru; Наличие базы данных электронного каталога – Фолиант.
- Пакет программ MicrosoftOffice;
- MathCAD;
- AutoCAD.

Информационные справочные системы:

- Компьютерная справочно-правовая система «Гарант».
- Электронная информационно-образовательная среда Е-кампус.

Перечень программного обеспечения и информационных справочных систем

1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях (рег. номер 9334708), AutoCAD 2015 (бесплатный для вузов), Embarcadero rad studio - Г/к 445/01 от 30 июля 2010 г., IBM Rational Rose modeler (бесплатно по программе IBM Academic Initiative), Mathcad Education - University Edition (50 pack) -договор № 24-эа/15 от 19 августа 2015г., Microsoft Office - №61541869, Cisco Packet Tracer - договор № 23-с от 27 июня 2012 г., Microsoft Windows 7 Профессиональная - №61541869, Visual Studio IDE – AzureDev ID: a6c2b0d7-162e-479f-8a58-384701f33665, Microsoft Visual Basic – AzureDev ID: a6c2b0d7-162e-479f-8a58-384701f33665, Microsoft SQL Server – AzureDev ID: a6c2b0d7-162e-479f-8a58-384701f33665, PascalABC.NET (бесплатный), Oracle VM VirtualBox (бесплатный).

15. Описание материально-технической базы, необходимой для проведения практики

Определяется структурой места прохождения практики, если практика проходит на кафедре ВУЗа используется следующее материально-техническое обеспечение: специализированная учебная мебель и технические средства обучения, служащие для представления учебной информации: компьютеры (5 шт) с подключением к сети "Интернет" и доступом в электронную информационно-образовательную среду, книжные шкафы для учебной литературы и учебно-методических материалов